

# CLAIMS

What is claimed is:

504  
AL

1. A method of authenticating a subject, comprising:  
 2 using one or a plurality of biometric measurements for authentication  
 3 without any sharing of the subject's biometric data.
- 1 2. The method according to claim 1, further comprising:  
 2 storing said biometric data in an individual unit, said individual unit  
 3 belonging to said subject.
- 1 3. The method according to claim 2, wherein said individual unit is portable  
 2 for being carried by said subject.
- 1 4. The method according to claim 2, wherein said individual unit is non-  
 2 portable.
- 1 5. The method according to claim 2, wherein said individual unit comprises  
 2 one of a smart card, a personal area network (PAN) tool, and an apparatus  
 3 linked to a network.
- 1 6. The method according to claim 1, further comprising:

2 after said authentication, selectively obtaining access to any of a  
3 location, a service, and an option in a service by said subject.

1 7. The method according to claim 1, further comprising:

2 generating at least one of a password and another authentication  
3 procedure based on biometric authentication locally under the subject's  
4 control.

1 8. The method according to claim 7, further comprising:

2 securely storing the biometric on an apparatus carried by said subject.

1 9. The method according to claim 1, further comprising:

2 generating at least one of a password and another authentication  
3 procedure based on at least one biometric feature extracted locally under the  
4 subject's control.

1 10. The method according to claim 9, wherein said generating is performed  
2 without storing the subject's biometric feature.

1 11. The method according to claim 9, further comprising:

2 deriving said at least one of the password and the another  
3 authentication procedure from the biometric extracted locally when  
4 authentication is required.

1 12. The method according to claim 7, further comprising:  
2 deriving said at least one of the password and the another  
3 authentication procedure from compressed biometrics extracted locally under  
4 the subject's control or from a network, when authentication is required.

1 13. The method according to claim 7, further comprising:  
2 managing multiple passwords and authentication procedures, by at  
3 least one of:  
4 monitoring an authentication request;  
5 identifying a requestor;  
6 generating at least one of a new password and an  
7 authentication procedure for a new requester;  
8 storing the authentication procedure generation method and  
9 the identity of the requestor in a secure manner; and  
10 authenticating the user for known requesters using the stored  
11 procedure and the result of the local authentication procedure.

1 14. A method of authenticating a characteristic of a subject, without  
2 compromising privacy of the subject, comprising:  
3 using at least one of a plurality of authentication methods including  
4 personal information of the subject, a biometric of the subject, a password, a  
5 personal identification number (PIN) and a secured component; and

6 simultaneously with said using, said subject maintaining  
7 confidentiality of authentication information and withholding said  
8 authentication information from the other party.

1 15. The method according to claim 14, further comprising:  
2 generating at least one of a password and another authentication  
3 procedure based on authentication locally under the subject's control.

1 16. The method according to claim 15, further comprising:  
2 securely storing authentication information on an apparatus locally  
3 under the subject's control.

1 17. The method according to claim 15, further comprising:  
2 deriving said at least one of the password and the another  
3 authentication procedure from the local authentication when authentication is  
4 required.

1 18. The method according to claim 16, further comprising:  
2 securely storing the authentication information on the apparatus using  
3 at least one of a knowledge-based information, a possession-based  
4 information, a password-based information, and a biometric-based  
5 information.

- 1 19. The method according to claim 14, further comprising:  
2 selectively completing the authentication with a remote service using  
3 a communication port and protocol.
- 1 20. A method for secure authentication of a subject, comprising:  
2 selectively requesting any of a password and a knowledge-based  
3 information from said subject; and  
4 simultaneously with said selectively requesting, interrogating  
5 biometric information of the subject, said biometric information being carried  
6 by said subject.
- 1 21. The method according to claim 20, further comprising:  
2 using said biometric information to generate said password.
- 1 22. The method according to claim 20, further comprising:  
2 performing biometric data verification by a device associated with  
3 said subject,  
4 wherein said biometric data verification activates a password-  
5 controlled authentication mechanism which transfers information, but which  
6 withholds sufficient information so that the biometric is not revealed, to a  
7 party requiring authentication.
- 1 23. The method according to claim 21, wherein obtaining said password is

2 performed by using at least one of an encryption and secure hashing.

1 24. The method according to claim 20, wherein a device is carried by the  
2 subject to be authorized to perform a task,  
3 wherein at a moment of authorization, said device is presented to a  
4 reader of an authorizing machine of an entity seeking authentication, which  
5 prompts said device for a password for authorization to be given, and  
6 wherein said device reads a biometric of said subject using a sensor  
7 included in the device and computes the password.

1 25. The method according to claim 24, wherein said device allows the  
2 password to be read by the authorizing machine.

1 26. The method according to claim 25, wherein said password is read in a  
2 contacting manner.

1 27. The method according to claim 25, wherein said password is read in a  
2 contact-free manner.

1 28. The method according to claim 24, further comprising:  
2 using one of a hashing and a mapping technique, which is stable with  
3 respect to variations of the biometric extracted, said using including mapping  
4 regions of a biometric-print space, to the password having been computed.

1 29. The method according to claim 28, wherein said using includes:  
2 measuring a biometric-print of the subject by ranking biometric prints  
3 of N subsets of M biometrics,  
4 wherein an index of a top ranking of each of the N subsets is used in  
5 computing the password.

1 30. The method according to claim 24, further comprising:  
2 storing on the device information regarding a previous authentication  
3 including a biometric-print of the subject.

1 31. The method according to claim 20, further comprising:  
2 encrypting a biometric-print using the subject's biometric and  
3 personal knowledge onto a device carried by said subject.

1 32. The method according to claim 20, further comprising:  
2 providing a unique non-duplicable authentication mechanism on a  
3 device associated with said subject, said authentication mechanism being  
4 constructed so as to be completely independent of the biometric,  
5 wherein said authentication mechanism is prevented from accessing  
6 the biometric itself.

1 33. The method according to claim 32, wherein said device associated with

2 said subject produces a correct password only when the device reads a  
3 biometric from the subject.

1 34. The method according to claim 20, wherein biometric information for a  
2 plurality of subjects is stored in a device associated with the subject.

1 35. An apparatus for secure authentication, without compromising privacy of  
2 a subject, comprising:

3 a reader, associated with the subject, for reading a specified biometric  
4 of said subject; and

5 a password generator for producing a password needed based on said  
6 biometric.

1 36. The apparatus according to claim 35, wherein said password generator  
2 includes an encryption device using at least one of encryption and secure  
3 hashing.

1 37. An apparatus for secure authentication, comprising:

2 means, associated with a subject, for reading a specified biometric of  
3 said subject; and

4 means for producing a password needed based on said biometric,  
5 without providing access to said biometric by anyone other than said subject.



1 38. The apparatus according to claim 37, wherein said means for producing  
2 said password includes an encryption device using at least one of encryption  
3 and secure hashing.

1 39. A method of identifying a subject, comprising:  
2 using one or a plurality of biometric measurements for identification  
3 without any sharing of the subject's biometric data.

1 40. The method of claim 39, wherein a subject's identity is determined  
2 locally, under the subject's control, by having the subject provide at least one  
3 of a user ID and by biometric identification of the subject among enrolled  
4 authorized subjects, and  
5 wherein said identification produces a set of N best matches for N  
6 subsets, and an index formed by concatenation of the N indices uniquely  
7 identifies the subject.

1 41. A method for identification of a subject, comprising:  
2 selectively requesting any of a password and a knowledge-based  
3 information from said subject; and  
4 simultaneously with said selectively requesting, interrogating  
5 biometric information of the subject, said biometric information being carried  
6 by said subject.

1 42. The method of claim 41, wherein a subject's identity is determined  
2 locally, under the subject's control, by having the subject provide at least one  
3 of a user ID and by biometric identification of the subject among enrolled  
4 authorized subjects, and

5 wherein said identification produces a set of N best matches for N  
6 subsets, and an index formed by concatenation of the N indices uniquely  
7 identifies the subject.

1 43. An apparatus for identification of a subject, comprising:

2 a reader, associated with the subject, for reading a specified biometric  
3 of said subject; and

4 a password generator for producing a password needed based on said  
5 biometric.

1 44. The apparatus according to claim 43, further comprising:

2 means for storing data of said biometric in an individual unit, said  
3 individual unit belonging to said subject.

1 45. The apparatus according to claim 44, wherein said individual unit is  
2 portable for being carried by said subject.

1 46. The apparatus according to claim 44, wherein said individual unit is non-  
2 portable.

1 47. The apparatus according to claim 44, wherein said individual unit  
2 comprises one of a smart card, a personal area network (PAN) tool, and an  
3 apparatus linked to a network.

1 48. The apparatus according to claim 44, wherein a subject's identity is  
2 determined locally, under the subject's control, by having the subject provide  
3 at least one of a user ID and by biometric identification of the subject among  
4 enrolled authorized subjects being read by said reader, and  
5 wherein said identification produces a set of N best matches for N  
6 subsets, and an index formed by concatenation of the N indices uniquely  
7 identifies the subject.

487